UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/940,035	08/27/2001	Lane W. Lee	M-12040 US	4896

32605 7590 03/24/2008

MACPHERSON KWOK CHEN & HEID LLP
2033 GATEWAY PLACE
SUITE 400
SAN JOSE, CA 95110

EXAMINER	
DINH, MINH	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
03/24/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/940,035	LEE ET AL.	
	Examiner	Art Unit	
	MINH DINH	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 November 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *25 and 26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *25 and 26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Art Unit: 2132

DETAILED ACTION

Response to Amendment

1. This action is in response to the RCE filed 11/30/2007.

Response to Arguments

2. Applicant's arguments filed 11/30/07 have been fully considered but they are not persuasive. Applicant argues that Mochizuki (7,020,780) teaches no encryption/decryption of the content by either the title key or the cipher key (page 3, 3rd paragraph). Although Mochizuki does not explicitly disclose encryption/ decryption of the content file, one of ordinary skill in the art would readily recognize that the feature is implied by the term "cipher key". Even if Mochizuki does not encrypt the content file with the keys, encrypting content is well known in the art, and it would have been obvious to encrypt Mochizuki's content file with the keys to prevent unauthorized access to the plaintext content file.

Applicant argues that Mochizuki does not teach writing the complement key to the disk (page 4, 3rd paragraph). Mochizuki discloses writing the complement key (i.e., the cipher key) on the disc (fig. 7, step S42; col. 10, lines 3-7).

Art Unit: 2132

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mochizuki (7,020,780) in view of Sims, III (6,550,011) and Shear et al. (2001/0042043). Mochizuki discloses a method of unlocking a locked file stored in mastered pre-recorded portion on a storage medium, wherein both a title key and a cipher key are needed to unlock the locked file, the title key and the cipher key being functionally equivalent to a content key and a complement key, the mastered pre-recorded portion including the title key but not the cipher key, the storage medium also having an writeable area that is writable by a storage engine, the method comprising: receiving a request from a host device at the storage engine to unlock the locked file; providing the storage engine with the cipher key; and writing the cipher key to the writeable area to unlock the file (Abstract; figures 6-7, 9; col. 8, lines 50-66; col. 10, line 26 – col. 11, line 17).

Mochizuki discloses using the title key and the cipher key to unlock the content file. Although Mochizuki does not explicitly disclose encryption/

decryption of the content file using the keys, one of ordinary skill in the art would readily recognize that the feature is implied by the term "cipher key". Even if Mochizuki does not encrypt the content file with the keys, Official Notice is taken that encrypting content is well known in the art, and it would have been obvious to encrypt Mochizuki's content file using the keys to prevent unauthorized access to the plaintext content file.

Mochizuki does not disclose authenticating a host device and authenticating the storage engine with a server. Sims discloses a method of unlocking locked content stored in a storage medium including the steps of authenticating a host device (col. 5, lines 39-59; col. 19, lines 29-49) and authenticating the storage engine with a server (col. 17, lines 1-23). It would have been obvious to modify the Mochizuki method to authenticate the host device and authenticate the storage engine with a server, as taught by Sims, in order to verify that the host device and the storage engine are both authorized devices.

Mochizuki discloses that the host device decrypts the file using the key provided by the engine. Mochizuki does not disclose that the engines itself decrypts the file and then provides the decrypted file content to the host. Shear discloses a secure storage engine (i.e., a disk drive) which decrypts file content and provides the decrypted file content to the host wherein decryption keys are never exposed outside of the engine (fig. 4A;

paragraphs 0081, 0219, 0250-0252). It would have been obvious to modify the Mochizuki method to such that the engines is a secure engine which decrypts the file and provides the decrypted file content to the host but does not expose the decryption keys outside of the engine, as taught by Shears, in order to provide an additional security layer.

5. Claim 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mochizuki in view of Sims and Shear as applied to claim 25 above, and further in view of Menezes et al ("Handbook of Applied Cryptography"). Sims discloses authenticating the host device requiring two passes (i.e., two messages to be transmitted), but Sims does not disclose using one-pass protocol in which a first entity who generates the random session key is also the entity that encrypts the session key with a second entity's public key and transmits the encrypted session key to the second entity participating in a communication session. Menezes discloses using one-pass protocol for transporting a session key and for implicit key authentication (Section 12.5.1, page 507-508). It would have been obvious to modify the combined method of Mochizuki, Sims and Shear to authenticate the host device using one-pass protocol, as taught by Menezes, in order to reduce network traffic.

Art Unit: 2132

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MINH DINH whose telephone number is (571)272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Art Unit: 2132

/M. D./
Examiner, Art Unit 2132

3/16/08

/Benjamin E Lanier/
Primary Examiner, Art Unit 2132